Is VPN the ideal set-up for remote working?

The pandemic has propelled many businesses and organisations to fully embrace remote working as one of the most essential capabilities they need to establish. In many cases this is to enable employees to work from home or in fact, anywhere they are, even if they are stranded overseas due to border closures.

The problem is how to do this cost-effectively and securely.

The common practice would be to set up a secure Virtual Private Network (VPN) that extends to each and every remote employee's workstation, be it a desktop or laptop. This grants that employee access to the organisation's private network so that he or she could use resources on the intranet and transfer data to and from business applications. Such a VPN is typically set-up and maintained by IT professionals, whether in-house or outsourced as the complexity is beyond a non-technical person.

While this practice is the standard go-to for many small to medium organisations, is it really ideal in every scenario?

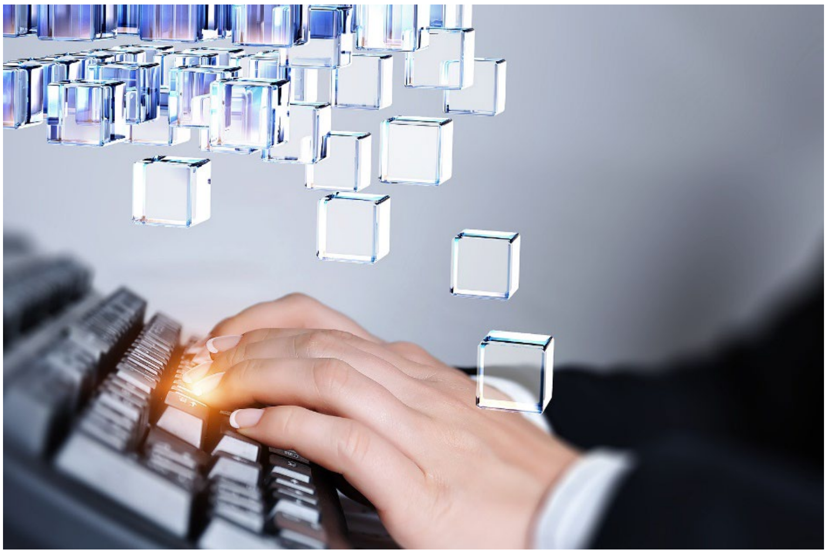
Let's consider first the cost. As a business you will need to enlist the help of IT professionals or at least someone with enough technical capability. An average salary of circa $80k to $100k p.a. or perhaps a monthly reoccurring managed IT service fee if outsourced. Then there is the licensing fee for every employee who needs to use your business applications, regardless of how frequent that is. What if you need to only temporarily hire someone? Do you still set up a VPN access and purchase user licence?

The licencing fee is especially worth some attention because it leads to the notion of over-subscribing resources that would only be used infrequently. For instance, a sales person who needs to log on once a day or perhaps a contractor who needs to access only when there is a job. Do they need a full user licence for the kinds of business applications they need? But then would the return justify for that user licence given the low usage?

This is where I think a remote desktop protocol (RDP) solution such as MoxyViewer would make more sense. The difference between RDP and VPN is that the user gains access to a desktop or laptop environment on another machine via the RDP. Put simply the user not only sees the remote desktop but also can control that remote desktop. VPN on the other hand is connecting the user's own machine into the network, instead of letting the user see and control another one.

So why does RDP solutions like MoxyViewer makes sense where VPN doesn't?

It comes down to being cost-effective. In the example of those employees with low usage of applications, they could potentially connect to one machine already set up in the main office via RDP. Using this particular machine, these users can do what they need to do instead of needing a VPN or a separate user licence.



This is also one of the main reasons of why we built the MoxyViewer product. Our original cohort of users were staff and students of tertiary education institutions who needed to access highly specialised applications for learning and research purposes. It was impossible to expect each and everyone of them to purchase a separate user licence. It was simply uneconomical for the level of usage. During the pandemic when they could not physically come onsite this problem became a burning issue. So MoxyViewer was created to solve it.

The same problem of high cost but low usage is prevalent in the business community. Perhaps now is the time for a rethink.